UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/658,310	09/09/2003	Ed H. Frank	14177US02	2145

23446 7590 10/30/2007
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
10/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	Application No.	Applicant(s)	
	10/658,310	FRANK ET AL.	
	Examiner	Art Unit	
	Carlton V. Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Applicant's submission filed on 8/22/2007 has been entered.

2. This action is responding to application papers filed on **8-22-2007**. Claims **1 - 42** are pending. Claims **1, 15, 29** have been amended. Claims **1, 15, 29** are independent.

Response to Arguments

3. Applicant's arguments filed 8/22/2007 have been fully considered but they are moot based on new grounds of rejection.

In any event:

3.1 Within applicant's invention *"there is no disclosure that hosting said communication session over a third PHY channel" (not exclusively). (see amended claims 1, 15, 29)* The specification states that, *"A communication session may be hosted over the first PHY channel, the second PHY channel or a third PHY channel." (see specification paragraph [0020])* In addition, the specification states that, *"A third*

PHY channel or the first or second PHY channels may be adapted to host or facilitate the communication session." (see specification paragraph [0038]) There is no disclosure that a communication session is hosted over the third PHY channels exclusively. If applicant feels there is disclosure for this particular claims limitation, please feel to indicate the required citations for confirmation.

In any event, the Chandrashekhar prior art discloses a communication session hosted over a PHY channel. (see Chandrashekhar paragraph [0057], lines 1-5; paragraph [0062], lines 1-4: physical communications channel) A physical channel is a requirement in order to perform network communications between two network-connected endpoints. The Chandrashekhar prior art discloses that the hosted session can be over either one of multiple communications paths (channels) available to the prior art invention. (see Chandrashekhar paragraph [0040], lines 4-6; paragraph [0040], lines 9-11; paragraph [0075], lines 6-19: multiple (first, second, third) communications paths (PHY channels))

3.2 Applicant argues that the referenced prior art does not disclose, *" authenticating said originating access device ". (see Remarks Page 13)*

The Chandrashekhar prior art discloses an authentication procedure over network communications. The Chandrashekhar prior art discloses authentication using a first physical (PHY) channel for a request for VPN service and a second physical (PHY) channel for the authentication procedure. (see Chandrashekhar Figure 3; paragraph [0057], lines 1-5; paragraph [0062], lines 1-4) The VPN manager utilizes an authentication server, which is connected by a communications bus or communications

path and performs the authentication procedure. This is a different communications path than utilized for the request for VPN service from user1 to the VPN manager (enhanced application portal). The Chandrashekhar prior art discloses the claim limitation of a first channel for processing a request and a second channel for authentication.

In addition, the Chandrashekhar and Giniger prior art combination discloses authentication of a network device such as an originating access device. (see Giniger col. 3, lines 21-25: VPN (tunnel) communications; col. 4, lines 59-67; col. 5, lines 6-10; col. 15, lines 27-33: authentication, network device)

3.3 Applicant argues that the referenced prior art does not disclose, *" hosting said communication session over a third PHY channel ". (see Remarks Page 14)*

A physical communications path is a requirement to host a communications session. (see Chandrashekhar Figure 3; paragraph [0057], lines 1-5; paragraph [0062], lines 1-4: physical communications channel) The Chandrashekhar prior art discloses multiple communications paths available for access to the authentication server, to host a communications session, and for the secure transfer of security information (encryption/decryption keys). (see Chandrashekhar paragraph [0040], lines 4-6; paragraph [0040], lines 9-11: multiple (first, second, third) communications paths (PHY channels))

3.4 The examiner has considered the applicant's remarks concerning multiple encryption in a multi-band, multi-protocol hybrid wired/wireless network including

receiving on a first PHY channel of an access point, a request for initiation of a communication session. The received request may be acknowledged on the first PHY channel and the originating access device may be authenticated on a second PHY channel. A third PHY channel or the first or second PHY channels may host the communication session. One or more encryption/decryption keys may be provided via the first PHY channel or the second PHY channel for use during the communication session. The authentication information may be requested and delivered to the originating access device via a second PHY channel. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Chandrashekhar (20030140131), Giniger (6,751,729) and He (6,088,451) discloses applicant's invention including disclosures in Remarks dated August 22, 2007.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 6 - 9, 12 - 15, 20 - 23, 26 - 29, 34 - 37, 40 - 42** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chandrashekhar et al.** (US PGPUB No. **20030140131**) in view of **Giniger et al.** (US Patent No. **6,751,729**).

Regarding Claims 1, 15, 29, Chandrashekhar discloses a method, machine-readable storage having stored upon a computer program having at least one code section, system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising: receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device; authenticating said communication session by authenticating said access using a second PHY channel; and hosting said communication session over a third PHY channel. (see Chandrashekhar paragraph [0054], lines 3-5; paragraph [0054], lines 10-12: hybrid communications network; paragraph [0040], lines 4-6; paragraph [0108], lines 1-5: wireless/wired communications; paragraph [0056], lines 1-3: request for communications service; paragraph [0048], lines 1-7: software, implementation means); Figure 3) Chandrashekhar does not specifically disclose whereby authenticating said originating access device. However, Giniger discloses wherein authenticating said originating access device. (see Giniger col. 3, lines 21-25: VPN (tunnel) communications; col. 4, lines 59-67; col. 5, lines 6-10; col. 15, lines 27-33: authentication, network device)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar as taught by Giniger to enable the capability to authenticate a network device (an originating access device). One of ordinary skill in the art would have been motivated to employ the teachings of Giniger in order to enable the capability for the selection of the optimum path based on security policy, setup conditions and routing

parameters to optimized bandwidth, save time, and reduce operating costs. (see Giniger col. 6, lines 31-38: " *... Dynamic routing enables the creation of meshed VPN network topologies. The optimum path is automatically selected based on security policy, setup connections, and routing parameters to optimize bandwidth, save time, and reduce operating costs. On a larger scale, users can form communities of interest by creating their own virtual networks within existing enterprise topologies using private or public networks. ...* ")

Regarding Claims 6, 20, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, comprising receiving an identification of said originating access device by said access point. (see Chandrashekhar paragraph [0073], lines 13-16: identification for originating device, user; paragraph [0037], lines 4-15: access network (i.e. access point))

Regarding Claims 7, 21, 35, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having one code section, system according to claims 6, 20, 34, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address. (see Chandrashekhar paragraph [0073], lines 13-16; paragraph [0082], lines 14-16: IP address utilized as identification)

Regarding Claims 8, 22, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, comprising acknowledging said received request on said first PHY channel. (see Chandrashekhar paragraph [0057], lines 3-7: response to received request (i.e. response, ACK))

Regarding Claims 9, 23, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, comprising determining a type of traffic generated by said originating access device on said first PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15: type of traffic, VPN; paragraph [0054], lines 7-12: between communications endpoints)

Regarding Claims 12, 26, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, further comprising establishing at least one virtual channel between said originating access device and a terminating access device. (see Chandrashekhar paragraph [0054], lines 7-12: establish circuit between originating device and terminating device (i.e. endpoints, communications circuit); paragraph [0040], lines 4-6: dial-up user, physical circuit))

Regarding Claims 13, 27, Chandrashekhar discloses the method, machine-readable

storage having stored upon a computer program having at least one code section according to claims 12, 26, comprises tunneling information between said originating access device and said terminating access device. (see Chandrashekhar paragraph [0032], lines 2-5; paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: tunneling between originating and termination devices (i.e. endpoints))

Regarding Claims 14, 28, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 12, 26, comprising establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15; paragraph [0054], lines 7-12: virtual channel between originating and terminating devices (i.e. VPN tunnel, virtual channel endpoints))

Regarding Claim 34, Chandrashekhar discloses the system according to claim 29, wherein said at least one receiver is adapted to receive an identification of said originating access device by said access point. (see Chandrashekhar paragraph [0073], lines 13-16: identification for originating device, user; paragraph [0037], lines 4-15: access network (i.e. access point))

Regarding Claim 36, Chandrashekhar discloses the system according to claim 29, wherein said at least one receiver is adapted to acknowledge said received request on

said first PHY channel. (see Chandrashekhar paragraph [0057], lines 3-7: response to received request (i.e. response, ACK))

Regarding Claim 37, Chandrashekhar discloses the system according to claim 29, wherein said at least one authenticator is adapted to determine a type of traffic generated by said originating access device on said first PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15: type of traffic, VPN; paragraph [0054], lines 7-12: between communications endpoints)

Regarding Claim 40, Chandrashekhar discloses the system according to claim 29, wherein at least one receiver is adapted to establish at least one virtual channel between said originating access device and a terminating access device. (see Chandrashekhar paragraph [0054], lines 7-12: establish circuit between originating device and terminating device (i.e. endpoints, communications circuit); paragraph [0040], lines 4-6: dial-up user, physical circuit))

Regarding Claim 41, Chandrashekhar discloses the system according to claim 40, wherein said at least one receiver is adapted to tunnel information between said originating access device and said terminating access device. (see Chandrashekhar paragraph [0032], lines 2-5; paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: tunneling between originating and termination devices (i.e. endpoints))

Regarding Claim 42, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 40, wherein said at least one receiver is adapted to establish at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel and/or said third PHY channel. (see Chandrashekhar paragraph [0028], lines 13-15; paragraph [0054], lines 7-12: virtual channel between originating and terminating devices (i.e. VPN tunnel, virtual channel endpoints))

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **2 - 5, 10, 11, 16 - 19, 24, 25, 30 - 33, 38, 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chandrashekhar-Giniger** and further in view of **He et al.** (US Patent No. **6,088,451**).

Regarding Claims 2, 16, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section

according to claims 1, 15. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0048], lines 1-7: software, implementation means) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein further comprising generating at least one encryption/decryption key for use during said communication session. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar as taught by He to enable the generation of an encryption/decryption key. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63: " ... *It also supports the implementation of network-wide centralized user administration and management, authentication, credential/privilege control and access to individual network elements, which is highly desirable for a large and complex network. ...* ")

Regarding Claims 3, 17, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 2, 17, wherein said authenticating comprises requesting authentication information from an authentication server. (see Chandrashekhar paragraph [0041], lines 1-5; paragraph [0057], lines 1-3: utilizing an authentication server for authorization)

Regarding Claims 4, 18, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 3, 17, wherein said authenticating comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel. (see Chandrashekhar paragraph [0057], lines 3-7: appropriate indication returned to user)

Regarding Claims 5, 19, 33, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 4, 18, 32. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints) Chandrashekhar does not specifically disclose delivering said encryption/decryption key. However, He discloses wherein comprising delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: delivering encryption/decryption key; Figure 3)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar as taught by He to enable the delivery of an encryption/decryption key. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

Regarding Claims 10, 24, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 9, 23, further comprising at least one key dependent on said determined traffic type. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0028], lines 13-15: virtual channel between originating and terminating device (i.e. VPN tunnel, virtual channel endpoints): key utilized for VPN type traffic, encryption key parameter) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein comprising generating at least one encryption/decryption key. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar as taught by He to enable the generation of an encryption/decryption key. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

Regarding Claims 11, 25, 39, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 10, 24, 38. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints)

Chandrashekhar does not specifically disclose the distribution of generated encryption/decryption key. However, He discloses wherein comprising distributing said generated at least one encryption/decryption key via at one or both of said second PHY channel and/or said third PHY channel. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: delivering (i.e. distributing) generated encryption/decryption key; Figure 3)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar as taught by He to enable the generation of an encryption/decryption key. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

Regarding Claim 30, Chandrashekhar discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claim 29. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0048], lines 1-7: software, implementation means) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein further comprising generating at least one encryption/decryption key for use during said communication session. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify

Chandrashekhar as taught by He to enable the generation of an encryption/decryption key. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

Regarding Claim 31, Chandrashekhar discloses the system according to claim 30, wherein said at least one authenticator is adapted to request authentication information. (see Chandrashekhar paragraph [0041], lines 1-5; paragraph [0057], lines 1-3: utilizing an authentication server for authorization)

Regarding Claim 32, Chandrashekhar discloses the system according to claim 31, wherein said authenticator is adapted to deliver at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel. (see Chandrashekhar paragraph [0057], lines 3-7: appropriate indication returned to user)

Regarding Claim 38, Chandrashekhar discloses the system according to claims 37, wherein said at least one authenticator is adapted further comprising at least one key dependent on said determined traffic type. (see Chandrashekhar paragraph [0054], lines 7-12; paragraph [0081], lines 7-9: communications between endpoints; paragraph [0028], lines 13-15: virtual channel between originating and terminating device (i.e. VPN tunnel, virtual channel endpoints): key utilized for VPN type traffic, encryption key

parameter) Chandrashekhar does not specifically disclose generating at least one encryption/decryption key. However, He discloses wherein said at least one authenticator is adapted to generate at least one encryption/decryption key. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify Chandrashekhar as taught by He to enable the generation of an encryption/decryption key. One of ordinary skill in the art would have been motivated to employ the teachings of He in order to a network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

C.J.

CVJ
October 15, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/26/07